

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Nobuo SAKIYAMA, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: COMMUNICATION GATEWAY APPARATUS, COMMUNICATION GATEWAY METHOD, AND  
PROGRAM PRODUCT

**REQUEST FOR PRIORITY**

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-096946	March 31, 2003
Japan	2003-400724	November 28, 2003

Certified copies of the corresponding Convention Application(s)

- are submitted herewith
- will be submitted prior to payment of the Final Fee
- were filed in prior application Serial No. filed
- were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- (B) Application Serial No.(s)  
 are submitted herewith  
 will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland  
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

0381872 2/2

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2003年 3月31日

出願番号 Application Number: 特願2003-096946

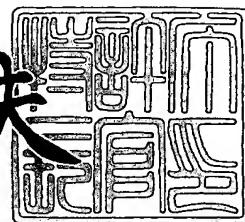
[ST. 10/C]: [JP2003-096946]

出願人 Applicant(s): 株式会社東芝

2004年 2月 3日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2004-3005439

【書類名】 特許願  
【整理番号】 A000300197  
【提出日】 平成15年 3月31日  
【あて先】 特許庁長官 殿  
【国際特許分類】 H04L 12/00  
【発明の名称】 通信中継装置、通信中継方法及びプログラム  
【請求項の数】 19  
【発明者】  
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内  
【氏名】 崎山 伸夫  
【発明者】  
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内  
【氏名】 吉田 英樹  
【特許出願人】  
【識別番号】 000003078  
【氏名又は名称】 株式会社 東芝  
【代理人】  
【識別番号】 100058479  
【弁理士】  
【氏名又は名称】 鈴江 武彦  
【電話番号】 03-3502-3181  
【選任した代理人】  
【識別番号】 100091351  
【弁理士】  
【氏名又は名称】 河野 哲

**【選任した代理人】**

【識別番号】 100088683

**【弁理士】**

【氏名又は名称】 中村 誠

**【選任した代理人】**

【識別番号】 100108855

**【弁理士】**

【氏名又は名称】 蔵田 昌俊

**【選任した代理人】**

【識別番号】 100084618

**【弁理士】**

【氏名又は名称】 村松 貞男

**【選任した代理人】**

【識別番号】 100092196

**【弁理士】**

【氏名又は名称】 橋本 良郎

**【手数料の表示】**

【予納台帳番号】 011567

【納付金額】 21,000円

**【提出物件の目録】**

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信中継装置、通信中継方法及びプログラム

【特許請求の範囲】

【請求項 1】 サーバからクライアントへ転送されるコンテンツを受信する受信手段と、

受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出手段と、

前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断手段と、

前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする通信中継装置。

【請求項 2】 前記クライアント情報の転送を許可する転送先を示す転送許可情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先が、前記転送許可情報により示される送信先に該当するものでない場合に、前記コンテンツの転送を許可しないと判断することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 3】 前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先が複数存在する場合には、該複数の送信先の全てが前記転送許可情報により示される送信先に該当するものであるときのみ、前記コンテンツの転送を許可すると判断することを特徴とする請求項 2 に記載の通信中継装置。

【請求項 4】 前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項 2 に記載の通信中継装置。

【請求項 5】 前記転送許可情報は、前記転送を許可する転送先を示すURLのリストを含むものであることを特徴とする請求項 2 に記載の通信中継装置。

【請求項6】 前記転送許可情報は、前記転送を許可する転送先を示すURLの正規表現記述を含むものであることを特徴とする請求項2に記載の通信中継装置。

【請求項7】 前記抽出手段は、

前記コンテンツから予め定められた言語により記述されたスクリプトプログラムを検出する手段と、

前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項1に記載の通信中継装置。

【請求項8】 前記抽出手段は、

検出された前記言語により記述されたスクリプトプログラムが、前記機能を有しないと判断された場合に、該スクリプトプログラムが文書を生成するものか否かについて判断する手段と、

前記言語により記述されたスクリプトプログラムが文書を生成するものと判断された場合に、該スクリプトプログラムを実行する手段と、

前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出する手段とを更に備えたことを特徴とする請求項7に記載の通信中継装置。

【請求項9】 前記抽出手段は、

前記コンテンツから予め定められた言語により記述された文書を検出する文書検出手段と、

前記言語により記述された文書が検出された場合に、該文書から予め定められた言語により記述されたスクリプトプログラムを検出するスクリプトプログラム検出手段と、

前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項1に記載の通信中継装置。

【請求項10】 前記抽出手段は、

検出された前記言語により記述されたスクリプトプログラムが、前記機能を有

しないと判断された場合に、該スクリプトプログラムが文書を生成するものか否かについて判断する手段と、

前記言語により記述されたスクリプトプログラムが文書を生成するものと判断された場合に、該スクリプトプログラムを実行する手段とを更に備え、

前記スクリプトプログラム検出手段は、前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出することを特徴とする請求項9に記載の通信中継装置。

【請求項11】 前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツを前記クライアントへ向けて送信しないことを特徴とする請求項1に記載の通信中継装置。

【請求項12】 前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツの代わりに、エラー用コンテンツを前記クライアントへ向けて送信することを特徴とする請求項11に記載の通信中継装置。

【請求項13】 前記送信手段は、前記判断手段により許可しないと判断された場合には、その旨を通知するメッセージを、予め定められた管理者のアカウントに宛てて送信することを特徴とする請求項11に記載の通信中継装置。

【請求項14】 前記送信手段は、前記メッセージに、少なくとも前記コンテンツを附加して送信することを特徴とする請求項13に記載の通信中継装置。

【請求項15】 前記判断手段を除いて前記通信中継装置を第1の計算機上に構成するとともに、前記判断手段を第2の計算機上に構成することを特徴とする請求項1に記載の通信中継装置。

【請求項16】 前記サーバは、Webサーバであり、

前記クライアント情報は、前記クライアント上で実行中のWebブラウザに保持されているクッキー情報を含むものであることを特徴とする請求項1に記載の通信中継装置。

【請求項17】 前記サーバは、Webサーバであり、

前記通信中継装置を、前記Webサーバに含まれる機能拡張モジュールとして構成することを特徴とする請求項1に記載の通信中継装置。

【請求項18】 サーバからクライアントへ転送されるコンテンツを受信す

るステップと、

受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出するステップと、

前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断するステップと、

許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信するステップとを有することを特徴とする通信中継装置。

【請求項19】 コンピュータを通信中継装置として機能させるためのプログラムであって、

サーバからクライアントへ転送されるコンテンツを受信する受信機能と、

受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出機能と、

前記抽出機能により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断機能と、

前記判断機能により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信機能とを実現させるためのプログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、クライアントとサーバとの間で転送されるコンテンツを中継する通信中継装置、通信中継方法及びプログラムに関する。

##### 【0002】

##### 【従来の技術】

インターネットでのWebアクセスに用いられるプロトコルであるHTTPは、要求に応じてコンテンツを返すことで完結する単純なプロトコルであり複数の要求にまたがる状態を持たない。従って、そのままではWebサーバは各Webブラウザを区別することができない。一方、現実の応用では各Webブラウザを

区別して認証を行ったり複数のH T T P にまたがって状態を保持したセッションを維持したりする必要があり、このためにクッキー（C o o k i e）と呼ばれるメカニズムが用いられてきた。

#### 【0003】

クッキーはW e b サーバで任意に解釈できる文字列であり、W e b ブラウザからのH T T P による要求に対する応答のなかでW e b サーバから送信されてW e b ブラウザ中に設定され、W e b ブラウザが次回から同一W e b サーバ、ないし同一ドメインに属するW e b サーバへコンテンツを要求する際に、そのなかに埋め込まれてW e b サーバに送信される。クッキーが埋め込まれていない要求への返答に対してW e b サーバがそれぞれ異なるクッキー設定の返答を行うことで、W e b サーバは各W e b ブラウザを区別できることになる。

#### 【0004】

一方、W e b ブラウザで表示される文書の記述技術として、J a v a S c r i p t (TM) やV B S c r i p t (TM) といったスクリプト言語によって記述されたプログラムをH T M L 中に埋め込んで用いる方法が広く用いられている。W e b ブラウザで受信されたH T M L 文書は表示のため内部で解析されて構造を持ったオブジェクトとして扱われるが、このオブジェクトに対してイベントドリブンの操作をスクリプト言語で行うことで動的なコンテンツ表示を行うことを可能としている。これらのスクリプトプログラムはW e b サーバにより提供され異なる管理下にあるW e b ブラウザ上で実行される性質を持つため、通常の状態で操作可能なオブジェクトは表示されるコンテンツやW e b ブラウザのG U I 部品に限定されている。ここで、先に説明したクッキーはW e b サーバが設定するものであるため、スクリプトプログラムから自由に操作することができるよう定められている。よって、スクリプトプログラムによるクッキーへの操作によって、クッキー文字列を他のドメインの提携サイトへと転送することによって新たな認証作業をW e b ブラウザのユーザが行わずにすむシングルサインオンも実装され得る。

#### 【0005】

また、W e b ブラウザとW e b サーバのそれぞれの所有者が特別な関係にありW e b サーバを「信頼できる」と判断する場合、W e b ブラウザの設定により特

定のWebサーバからのスクリプトプログラムによってWebブラウザの外のクライアント計算機上のリソースに対する操作を許可することができる。

#### 【0006】

以上のような技術的背景に対するセキュリティ上の脅威として、クロスサイトスクリプティング脆弱性と呼ばれる問題が知られている（例えば、非特許文献1参照）。クロスサイトスクリプティングとは、ユーザが閲覧するWebページに不正なスクリプトプログラムを混入させてユーザのWebブラウザで実行させることで、Webブラウザのクッキーが攻撃者サーバへ漏洩するなどセキュリティ上の被害が発生するものであり、そのような攻撃が有効となるWebシステムはクロスサイトスクリプティング脆弱性を有するとされる。

#### 【0007】

クロスサイトスクリプティング脆弱性の原因は、Webサイトでの動的ページ生成において、ユーザからの入力に由来する内容について十分なチェックが行われていないことにあり、チェックを行ない不正スクリプトの無効化を完全に行なうことが対策とされている（例えば、非特許文献1参照）。

#### 【0008】

しかし、平均的なWebサイト構築者にとって対策は困難な問題となっている（例えば、非特許文献2参照）。Webサイト構築に用いられるアプリケーションやミドルウェアが脆弱である場合、それらを組み合わせたり設定したりするだけでサイトを運営する場合は脆弱性をチェックするだけの技術をサイト構築者が持たない場合も多く、また仮にWebサイトを構築するプログラムを全て検査しようとした場合、検査項目が膨大になる場合が多いためである。

#### 【0009】

インターネットに接続する計算機の代表的なセキュリティ防護装置としてはファイアウォールが知られているが、クロスサイトスクリプティングはHTTPプロトコル中の形式的には正当なデータによる攻撃であるため、Webサーバを保護するためのファイアウォールによって防ぐことができない。

#### 【0010】

より高度な防御方法としては、侵入検知システムを設置しHTTPのリクエス

ト内容を細かく検査する方法がある（例えば、非特許文献3、4参照）が、クロスサイトスクリピティング脆弱性は特定少数の実装がほとんどとなるWebサーバの脆弱性だけではなく、多くのベンダが異なる実装を提供しているミドルウェアさらに個別サイトごとに作られたWebアプリケーションといった広範な領域に関係するため、完全に有効なルールセットを個別サイトの運営に関わらないベンダが提供するのは不可能であり、また個別サイトにとっても網羅的な検査ルールの作成は脆弱性そのものの除去と同程度のコストがかかると考えられる。

#### 【0011】

ユーザ側での自衛手段として、Webブラウザでのスクリプトプログラム実行全てを禁止する方法があるが、これらはWebサイトの正規のスクリプトプログラムの実行をも禁止するものである上、クロスサイトスクリピティング脆弱性の問題はWebサイト運営上の瑕疵によって生ずるものなので問題の解決とならない。

#### 【0012】

クロスサイトスクリピティングによる被害はクッキー漏洩に留まらず、クッキーの予期しない廃棄やWebサーバを「信頼できるサイト」と設定していた場合のクライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示などがあげられるが、なかでもクッキーは多くの電子商取引サイトでセッション保持や認証のために利用されており、その漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。従って、クッキーの漏洩に注目して対策することは有効である。

#### 【0013】

クッキー漏洩に着目すると、クライアント計算機上にソフトウェアで構成されたファイアウォールによってクッキーの送出を阻止する方法も存在している（例えば、非特許文献5）。しかし、Webサイトの正規のスクリプトプログラムの実行を妨害するものである上、クロスサイトスクリピティング脆弱性の問題はWebサイト運営上の瑕疵によって生ずるものなので、問題の解決とならない。

#### 【0014】

クッキー漏洩へのWebサイトとWebブラウザ双方で連携して行う対策とし

て、WebサーバでクッキーにHTTP-only属性を設定し、WebブラウザでスクリプトプログラムでのHTTP-only属性のついたクッキーの取扱いを禁止するという方式が提案されている（例えば、非特許文献6参照）。しかし、ユーザ側でのWebブラウザの更新が前提とされていること、正当な理由があってスクリプトによってクッキーを操作する場合には利用できない問題がある。

#### 【0015】

##### 【非特許文献1】

「セキュアプログラミング講座 A. WEBプログラマコース」、情報処理振興事業協会 セキュリティセンター、2001年

#### 【0016】

##### 【非特許文献2】

「クロスサイトスクリピティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」、高木浩光 関口智嗣 大蒔和仁、情報処理学会 第4回コンピュータセキュリティシンポジウム、2001年

#### 【0017】

##### 【非特許文献3】

Abstracting Application-Level Web Security, David Scott and Richard Sharp, the 11th International World-Wide Web conference (WWW2002), 2002

#### 【0018】

##### 【非特許文献4】

AppShield white paper, Sanctum Inc., 2001

#### 【0019】

##### 【非特許文献5】

シマンテック 2001年9月18日 プレスリリース, <http://www.symantec.co.jp/region/jp/news/year01/010918.html>, 株式会社シマンテック

#### 【0020】

##### 【非特許文献6】

Mitigating Cross-site Scripting With HTTP-only Cookies, Microsoft, 200

2, [http://msdn.microsoft.com/workshop/author/dhtml/httponly\\_cookies.asp](http://msdn.microsoft.com/workshop/author/dhtml/httponly_cookies.asp)

### 【0021】

#### 【発明が解決しようとする課題】

クロスサイトスクリピング脆弱性を悪用したクッキーに代表されるWebブラウザに格納される情報の漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。責任を負うべきWebサイト管理者にとって、事前に全ての脆弱性を検査して取り除くことは困難である。さらに、既存の脆弱性防御技術によってWebスクリピングの有用性を損なうことなく完全に対策を行うことは、Webアプリケーションからの脆弱性の完全な除去と同程度に困難であった。

### 【0022】

本発明は、上記事情を考慮してなされたもので、サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することのできる通信中継装置、通信中継方法及びプログラムを提供することを目的とする。

### 【0023】

#### 【課題を解決するための手段】

本発明に係る通信中継装置は、サーバからクライアントへ転送されるコンテンツを受信する受信手段と、受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出手段と、前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断手段と、前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする。

### 【0024】

好ましくは、前記クライアント情報の転送を許可する転送先を示す転送許可情報を記憶する記憶手段を更に備え、前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先が、前記転送許可情報に

より示される送信先に該当するものでない場合に、前記コンテンツの転送を許可しないと判断するようにしてもよい。

#### 【0025】

また、本発明に係る通信中継方法は、サーバからクライアントへ転送されるコンテンツを受信するステップと、受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出するステップと、前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断するステップと、許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信するステップとを有することを特徴とする。

#### 【0026】

また、本発明は、コンピュータを通信中継装置として機能させるためのプログラムであって、サーバからクライアントへ転送されるコンテンツを受信する受信機能と、受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出機能と、前記抽出機能により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断機能と、前記判断機能により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信機能とを実現させるためのプログラムである。

#### 【0027】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読み取り可能な記録媒体としても成立する。

#### 【0028】

本発明では、通信中継装置は、例えば、クライアント（ソフト的には、例えば、Webブラウザ）からの要求を受け付け、サーバ（例えば、Webサーバ）に転送する。サーバから要求に対応するコンテンツが返信されると、例えば、コンテンツのデータタイプを判定するなどして、スクリプトを含み得るデータタイプのものについてはスクリプトを抽出し、検査する。そして、例えば、クライアント情報（例えば、クッキーないしクッキーに由来するデータ等）の転送を試みるスクリプトが含まれると判定された場合、クライアント情報の転送先をアクセス制御リストと照合するなどして、転送を許可されない転送先（例えば、リストに含まれない転送先）である場合には、コンテンツのクライアントへの送信を禁止する。

### 【0029】

本発明によれば、クライアントに格納される情報の転送を試みる不正スクリプトがサーバからクライアントへ転送されることを防止でき、これによって、該不正スクリプトによりクライアントに格納される情報が漏洩されること防止することができる。また、この結果、例えばWebサーバ運営者の責任となるセキュリティ被害を防止することができる。さらに、例えば、送信を防止されたスクリプトを含むHTTPセッションについてWebサーバ管理者へ詳細を通知するなどが可能になるため、クロスサイトスクリプティング脆弱性をもつWebアプリケーションやミドルウェアについて修正やアップグレードなどの対策が容易になる。

### 【0030】

#### 【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

### 【0031】

以下では、通信中継装置としてネットワーク側通信インターフェースとWebサーバ側通信インターフェースがそれぞれ通信端点となり通信内容を転送するプロキシサーバの形態をとる場合を例にとって説明する。

### 【0032】

図1に、本発明の一実施形態に係る通信システムの構成例を示す。図1において

て、1はWebサーバ、2はクライアント計算機、21はクライアント計算機2上で動作するWebブラウザ、3はプロキシサーバ（通信中継装置）、8はネットワーク（本具体例では、インターネットとする）を示す。

#### 【0033】

図1では、1つのWebサーバのみ示しているが、複数のWebサーバが存在し得る。同様に、クライアント計算機2も複数存在し得る。

#### 【0034】

プロキシサーバ3とWebサーバ1との対応関係については、1つのプロキシサーバ2が唯一のWebサーバ1を対象とする構成と、1つのプロキシサーバ3が複数のWebサーバ1を対象にし得る構成とが可能である。

#### 【0035】

図2に、本実施形態のプロキシサーバの構成例を示す。

#### 【0036】

図2に示されるように、本プロキシサーバ3は、（要求元のクライアント計算機2上で動作する）Webブラウザとの通信を行うネットワーク側通信インターフェース31、Webサーバ1との通信を行うWebサーバ側通信インターフェース32、コンテンツ分類部33、文書解釈部34、スクリプト検査部35を備えている。

#### 【0037】

また、スクリプト検査部35は転送許可判定部351を有し、転送許可判定部351は転送許可リスト3511を有する。図3に、転送許可リスト3511の一例を示す。

#### 【0038】

なお、図1では、Webサーバ1とプロキシサーバ3とは、直接接続されるよう記述されているが、インターネットを介して接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。また、図1では、Webサーバ1とネットワーク8とは、直接接続されるよう記述されているが、例えば、インターネット経由で接続可能な他の中継装置を介して接続されてもよい。

**【0039】**

本プロキシサーバは、例えば、計算機によって実現することが可能である。

**【0040】**

以下、本実施形態の動作の概要について説明する。

**【0041】**

Webブラウザ（図1のクライアント計算機2参照）は、ネットワーク側通信インターフェース31にTCP/IPにより接続し、HTTPによるリクエストを送信する。本プロキシサーバ3のネットワーク側通信インターフェース31によつて受信されたリクエストは、Webサーバ側通信インターフェース32を経由してそのままWebサーバ1へ送られる。Webサーバ1では、リクエストに対応したレスポンスを本プロキシサーバ3のWebサーバ側通信インターフェース32へ送信する。本プロキシサーバ3のWebサーバ側通信インターフェース32では、コンテンツをコンテンツ分類部33へ送る。コンテンツ分類部33では、データ型に応じてスクリプトが含まれ得る型の文書とスクリプトが含まれる可能性がないデータに分類し、スクリプトが含まれる可能性がないデータについてはネットワーク側通信インターフェース31経由でWebブラウザに返信する。スクリプトが含まれ得る型の文書については、各データ型に対応する文書解釈部34へ送る。ただし、文書がスクリプトそのものである場合にはスクリプト検査部35へ送る。

**【0042】**

本プロキシサーバ3の文書解釈部34では、文書を構文解析する。構文解析の結果、スクリプトを含まない場合は、ネットワーク側通信インターフェース31経由でWebブラウザに返信する。スクリプトを含んでいる場合は、スクリプト検査部35へ送る。スクリプト検査部35では、スクリプトを検査し、Webブラウザに格納される情報に依存するいずれかのデータについて転送を試みるプログラムがあるかどうかを検査し、転送が行われ得る場合には、転送許可判定部351によって転送が許可されるかどうかを判別する。ここでは、転送許可判定部351は、転送先一覧をURLとして保持した転送許可リスト3511を転送許可規則とし照合するものとする。許可されない転送を含む場合は、エラーをネット

ワーク側通信インターフェース31経由でWebブラウザに送信する。さらに、スクリプトによって動的に文書が生成されるかどうか検査し、動的に文書が生成される場合には、文書解釈部34に結果を送って検査をやり直す。許可されない転送を含まない場合にのみ、スクリプト検査部35はネットワーク側通信インターフェース31経由でWebサーバ1からのレスポンスをWebブラウザへ返信する。

#### 【0043】

以下では、本実施形態のより詳細な動作例について説明するのに先立って、クロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

#### 【0044】

なお、ここでは、Webブラウザに格納される情報の一例としてクッキーを考えるものとする。

#### 【0045】

まず、図4を参照しながら、クッキーの典型的利用形態について説明する。図4は、本プロキシサーバにより転送許可される場合である。図4では、本プロキシサーバは省略している。なお、図4では、Webサイトの一例としてオンラインショップを示している（後掲の図5及び図6の同様である）。

#### 【0046】

(1) まず、クライアント計算機から所望のWebサーバへのアクセス・認証がなされる。

(2) 次に、Webサーバからクライアント計算機へ認証用クッキー設定要求がなされる。

(3) 次に、クライアント計算機においてクッキーの設定がなされる。

(4) そして、クライアント計算機からWebサーバへのクッキーつきアクセスがなされる。

#### 【0047】

これによって、WebサーバはWebブラウザを特定する必要のあるサービスを提供できるようになる。

#### 【0048】

次に、図5を参照しながら、提携サイトへのクッキー転送例について説明する。図5は、本プロキシサーバにより転送許可される場合である。図5では、本プロキシサーバは省略している。

#### 【0049】

(1) まず、クライアント計算機とWebサーバAとの間で、図4の(1)～(4)がなされる。

#### 【0050】

(2) 次に、WebサーバAからクライアント計算機へ「提携サイトBへのクッキー転送スクリプト」の送信がなされる。

#### 【0051】

(3) 次に、クライアント計算機において「提携サイトBへのクッキー転送スクリプト」が実行され、実行されたスクリプトによって、クライアント計算機からWebサーバBへのクッキー情報の転送・シングルサインオンがなされる。

#### 【0052】

このように、スクリプトプログラムによるクッキーへの操作によって、クッキー情報を他のWebサーバへ転送させ、例えば、新たな認証作業をWebブラウザのユーザが行わずにすむシングルサインオンなどができるようになる。

#### 【0053】

次に、図6を参照しながら、従来の通信システムにおけるクロスサイトスクリピティング脆弱性によるクッキー漏洩について説明する。

#### 【0054】

クロスサイトスクリピティングでは、図5で説明したような仕組みを悪用して、例えば、ユーザが閲覧するWebページに不正なスクリプトプログラムを混入させてユーザのWebブラウザで実行させることで、Webブラウザのクッキー情報を攻撃者サーバへ漏洩させるなどの不正が行われ得る。そして、クッキー情報の漏洩に留まらず、クライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示なども発生し得る。この不正は、例えば、以下のようにして実現される。

#### 【0055】

ここで、図6のWebサーバは、脆弱性を持つものとする（なお、このWebサーバ自体は正当なものである）。また、クライアント計算機は、この脆弱性を持つWebサーバとの間で、例えば、図4のような手順を既に行っており、クッキーを設定しているものとする。

### 【0056】

(1) まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

(2) クライアント計算機のWebブラウザが、この不正コンテンツをレンダリングする。

(3) そして、クライアント計算機からWebサーバへ、例えば漏洩先サイトへのクッキー転送スクリプトのもととなるデータ等の不正データを含むGETリクエストを送出してしまう。

(4) このGETリクエストを受けたWebサーバは、誤った出力処理をしてしまう。

(5) この結果、不正スクリプト（漏洩先サイトへのクッキー転送スクリプト）つきHTMLを送付してしまう。

(6) この不正スクリプト（漏洩先サイトへのクッキー転送スクリプト）つきHTMLを受けたクライアント計算機のWebブラウザでは、この不正スクリプトすなわち漏洩先サイトへのクッキー転送スクリプトを実行してしまう。

(7) この結果、クライアント計算機から漏洩先サイトへのクッキー情報の不正転送がなされてしまう。

(8) このようにして、漏洩先サイトは、攻撃したクライアント計算機のクッキー情報を不正に取得することができる。

(9) これによって、漏洩先サイトは、例えば、攻撃したクライアント計算機になりすまして、先のWebサーバへアクセスすることができる。

### 【0057】

これに対して、本実施形態では、図6のWebサーバとインターネットとの間に存在するプロキシサーバにおいて、図6の(5)の不正スクリプトつきHTMLを遮断するようにし、これによって、クッキー情報等の漏洩を防止することが

できるようにしている。

#### 【0058】

以下、本実施形態のより詳細な動作例について説明する。

#### 【0059】

図7及び図8に、本実施形態のプロキシサーバ3の処理手順の一例を示す。

#### 【0060】

なお、ここでは一例として、スクリプトとしてJavaScript及びVBScriptを対象とし、スクリプトを含む可能性のある文書としてHTML、XML及びCSSを対象とするものとする。また、前述のように、Webブラウザに格納される情報の一例としてクッキーを考えるものとする。

#### 【0061】

Webブラウザ（図1のクライアント計算機2参照）からのリクエストが本プロキシサーバ3を経由してWebサーバ1に送られ、Webサーバ1からのレスポンスが本プロキシサーバ3で受信される（ステップS1）。

#### 【0062】

本プロキシサーバ3は、HTTPリクエストを受信すると、当該リクエストが設定されたWebサーバへのリクエストであることを確認した上で（ステップS2）、Webサーバ1へリクエストを送信し（ステップS3）、対応するWebサーバ1からのHTTPレスポンスを受信する（ステップS5）。

#### 【0063】

なお、この一連の過程でエラーが発生した場合は（ステップS2でNoの場合、ステップS4でNoの場合、ステップS6でNoの場合）、エラーコードとエラーメッセージの生成を行って（ステップS7）、Webブラウザへエラーを示すレスポンスを返す（ステップS8）。

#### 【0064】

さて、受信（ステップS5）したHTTPレスポンスがHTTPのMessage-Bodyを含んでいない場合は（ステップS8）、HTTPレスポンスをそのままWebブラウザに転送する形で返信する（ステップS9）。

#### 【0065】

次に、H T T P レスポンスの内容はコンテンツ分類部3 3 に送られる。

#### 【0 0 6 6】

コンテンツ分類部3 3 では、H T T P レスポンスのContent-Type ヘッダによって、コンテンツがJavaS cript 又はVB S cript の場合は（ステップS 1 0）、スクリプト検査部3 5 に、HTML, XML, CSS の場合には（ステップS 1 1）、文書解釈部3 4 へ送る。その他の場合は（ステップS 1 0 でNo かつステップS 1 1 でNo の場合）、Web サーバ1 からのH T T P レスポンスをそのままWeb ブラウザに転送する形で返信する（ステップS 2 1）。

#### 【0 0 6 7】

文書解釈部3 4 では、文書の型に応じた構文解析を行い（ステップS 1 2）、文書がJavaS cript 又はVB S cript のスクリプトを含む場合は（ステップS 1 3）、スクリプト検査部3 5 へ送る。スクリプトを含まない場合は（ステップS 1 3）、Web サーバからのH T T P レスポンスをそのままWeb ブラウザに転送する形で返信する（ステップS 2 1）。

#### 【0 0 6 8】

スクリプト検査部3 5 では、スクリプトの構文解析および意味解析を行い、スクリプトで扱うオブジェクトの依存ツリーを作成する（ステップS 1 4）。

#### 【0 0 6 9】

依存ツリー中でDocument オブジェクトのCookie プロパティが参照され（ステップS 1 5）、かつ、当該クッキーに依存するデータが別のドキュメントのURL やForm のデータとされている場合（ステップS 1 6）、これらのURL について転送許可判定部3 5 1において転送許可リスト3 5 1 1 の内容と合致するかどうか検査する。なお、オブジェクトの依存ツリーに対して定数の畳み込みを行っても問題のURL を列挙する形で確定できない場合には、任意のURL への転送であると仮定して検査する（この場合、任意の転送先に対する転送が許可されていないならば、許可されないと判断する）。

#### 【0 0 7 0】

検査においてひとつでも許可リストに合致しないURL がクッキー転送に用い

られ得ると判断された場合には（ステップS17）、当該Webコンテンツについては転送が許可されないと判断して、当該WebコンテンツのWebブラウザ（クライアント計算機2）への送出を禁止し、検出された当該Webコンテンツに係るWebブラウザからの要求及び当該コンテンツを保存して、Webサーバ管理者への通知を目的としたログをとるとともに、該ログ（又は、当該コンテンツのみ若しくは当該要求のみ）を含む通知メッセージを作成し、事前に設定された管理者（アカウント）にメールで送信し（ステップS16）、またHTTPレスポンスについては、エラーコードとエラーメッセージを生成して（ステップS19）、Webブラウザへ返信する（ステップS21）。

#### 【0071】

スクリプト検査部35では、クッキーの検査とは別にDocumentオブジェクトのwriteメソッドが呼び出されているかどうかも検査する。Documentオブジェクトのwriteメソッドによって、Webブラウザによって解釈されるドキュメントが生成されるため、そのなかにスクリプトが含まれていれば実行される可能性があるためである。すなわち、ステップS15若しくはステップS16又はステップS17でNoとなったものについて、Documentオブジェクトのwriteメソッドが呼び出される場合には（ステップS14）、スクリプトを部分的に実行する形で新しい文書を作成し（ステップS21）、文書解釈部34へ処理を渡してスクリプトが含まれるかどうか検査するところに戻る。

#### 【0072】

以上のような検査をへてスクリプトがクッキーの不正転送を行わないと判断できる場合に、WebサーバからのHTTPレスポンスをそのままWebブラウザに転送する形で返信する。

#### 【0073】

このように本実施形態によれば、クッキー情報等の漏洩を防止することができる。

#### 【0074】

なお、上記では、当該Webコンテンツについて転送が許可されないと判断さ

れた場合に、当該WebコンテンツのWebブラウザ（クライアント計算機2）への送出を禁止するとともに、通知メッセージの送信や、エラーメッセージの送信を行ったが、通知メッセージの送信とエラーメッセージの送信の一方又は両方を行わない構成も可能である（ログを保存しない構成も可能である）。

#### 【0075】

なお、上記では、転送許可判定部351は、転送先一覧をURLとして保持した転送許可リスト3511を転送許可規則とし照合する場合を例にとって説明しているが、その代わりに、許可される転送先URLを正規表現の記述として保有し、個々の転送先URLと照合して全ての転送先URLが正規表現と一致する場合にのみ転送許可の結果を返すようにしてもよいし、両者を併用してもよい。

#### 【0076】

また、本プロキシサーバ（通信中継装置）は、1つの装置（例えば、計算機）で構成してもよいし、複数の装置（例えば、計算機）で構成してもよい。

#### 【0077】

後者の場合に、例えば、本プロキシサーバを構成する計算機から、転送許可判定部のみを独立させて、これをもう一つの計算機で構成するようにしてもよい。この場合、プロキシサーバ本体たる計算機と転送許可判定部たる計算機とは、例えば、専用線で接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。

#### 【0078】

また、上記の場合に、プロキシサーバ本体たる計算機と転送許可判定部たる計算機との対応関係については、1つの転送許可判定部たる計算機を唯一のプロキシサーバ本体たる計算機のみが使用可能とする構成と、1つの転送許可判定部たる計算機を複数のプロキシサーバ本体たる計算機が使用可能とする構成とが可能である。

#### 【0079】

また、これまでには、本プロキシサーバ（通信中継装置）とWebサーバとを別々の装置（例えば、計算機）で構成するものとして説明したが、例えば、本プロ

キシサーバ（通信中継装置）の不正コンテンツを遮断する機能に相当する部分（例えば、図2のコンテンツ分類部33、文書解釈部34、スクリプト検査部35、及びネットワーク側通信インターフェース31の機能のうちのエラーメッセージや通知メッセージ等を生成し送信する機能）の部分を、Webサーバに含まれる機能拡張モジュールとして実現することも可能である。また、この場合にも、上記のように、Webサーバ本体と転送許可判定部とを別々の計算機で実現するような構成も可能である。

#### 【0080】

また、上記では、ネットワークとしてインターネットを取り上げたが、もちろん、他のネットワークでも適用可能である。

#### 【0081】

また、上記では、スクリプトとしてJavaScripと及びVBScriptを対象とし、スクリプトを含む可能性のある文書としてHTML、XML及びCSSを対象とする場合を取り上げたが、もちろん、当該ネットワークで使用されるスクリプトあるいは不正に使用される可能性のあるスクリプトなど適宜の基準で対象とするスクリプトを選択して構わない。スクリプトを含む可能性のある文書についても同様である。また、新たなスクリプトや、スクリプトを含む可能性のある新たな文書が発生した場合には、それらを新たに対象として追加すればよい。

#### 【0082】

なお、以上の各機能は、ソフトウェアとして記述し適當な機構をもったコンピュータに処理させても実現可能である。

また、本実施形態は、コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるためのプログラムとして実施することもできる。加えて該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

#### 【0083】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階で

はその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

### 【0084】

#### 【発明の効果】

本発明によれば、サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することができる。

#### 【図面の簡単な説明】

【図1】 本発明の一実施形態に係る通信システムの構成例を示す図

【図2】 同実施形態に係る通信中継装置の構成例を示す図

【図3】 転送許可リストの一例を示す図

【図4】 クッキーの典型的利用形態について説明するための図

【図5】 提携サイトへのクッキー転送例について説明するための図

【図6】 クロスサイトスクリピング脆弱性によるクッキー漏洩及び同実施形態に係る通信中継装置による不正コンテンツの遮断によるクッキー漏洩の回避について説明するための図

【図7】 同実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

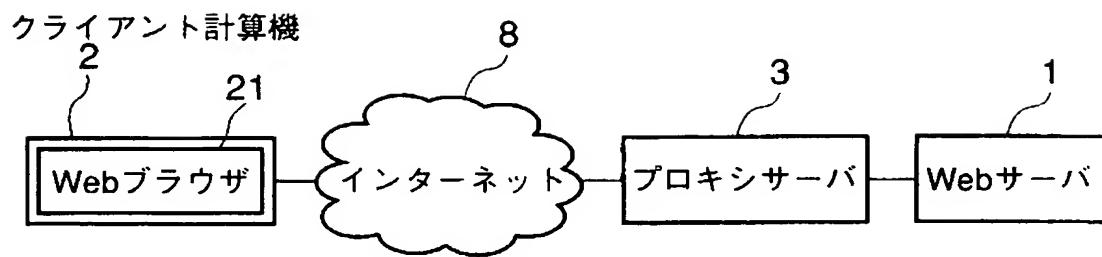
【図8】 同実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

#### 【符号の説明】

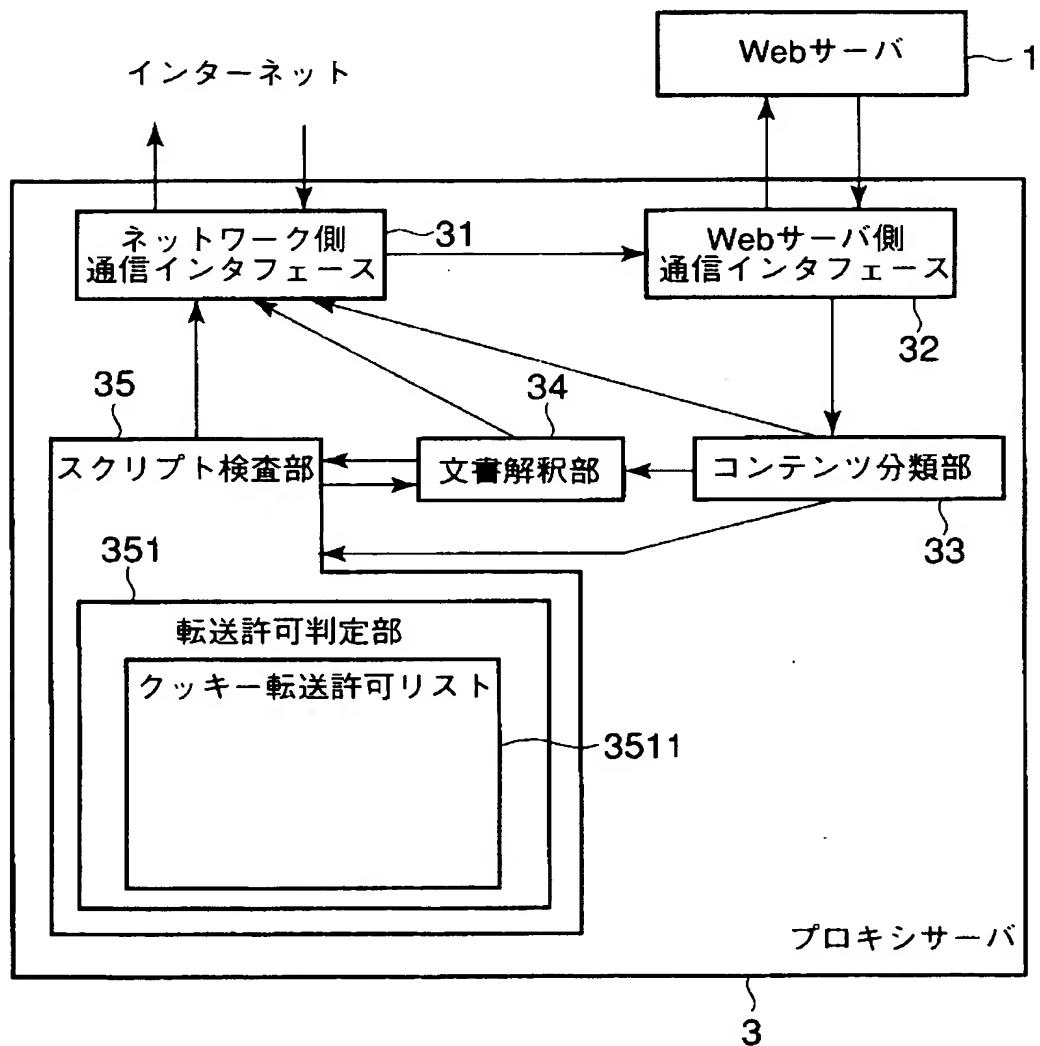
1…Webサーバ、2…通信中継装置、3…クライアント計算機、8…インターネット、21…Webブラウザ、31…ネットワーク側通信インターフェース、32…サーバ側通信インターフェース、33…コンテンツ分類部、34…文書解釈部、35…スクリプト検査部、351…転送許可判定部、3511…転送許可リスト

【書類名】 図面

【図 1】



【図 2】

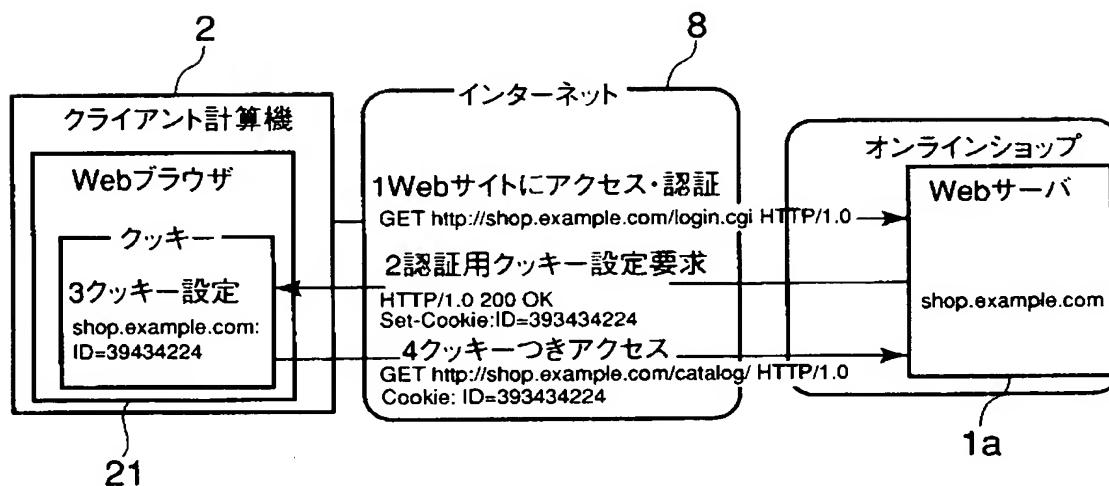


【図 3】

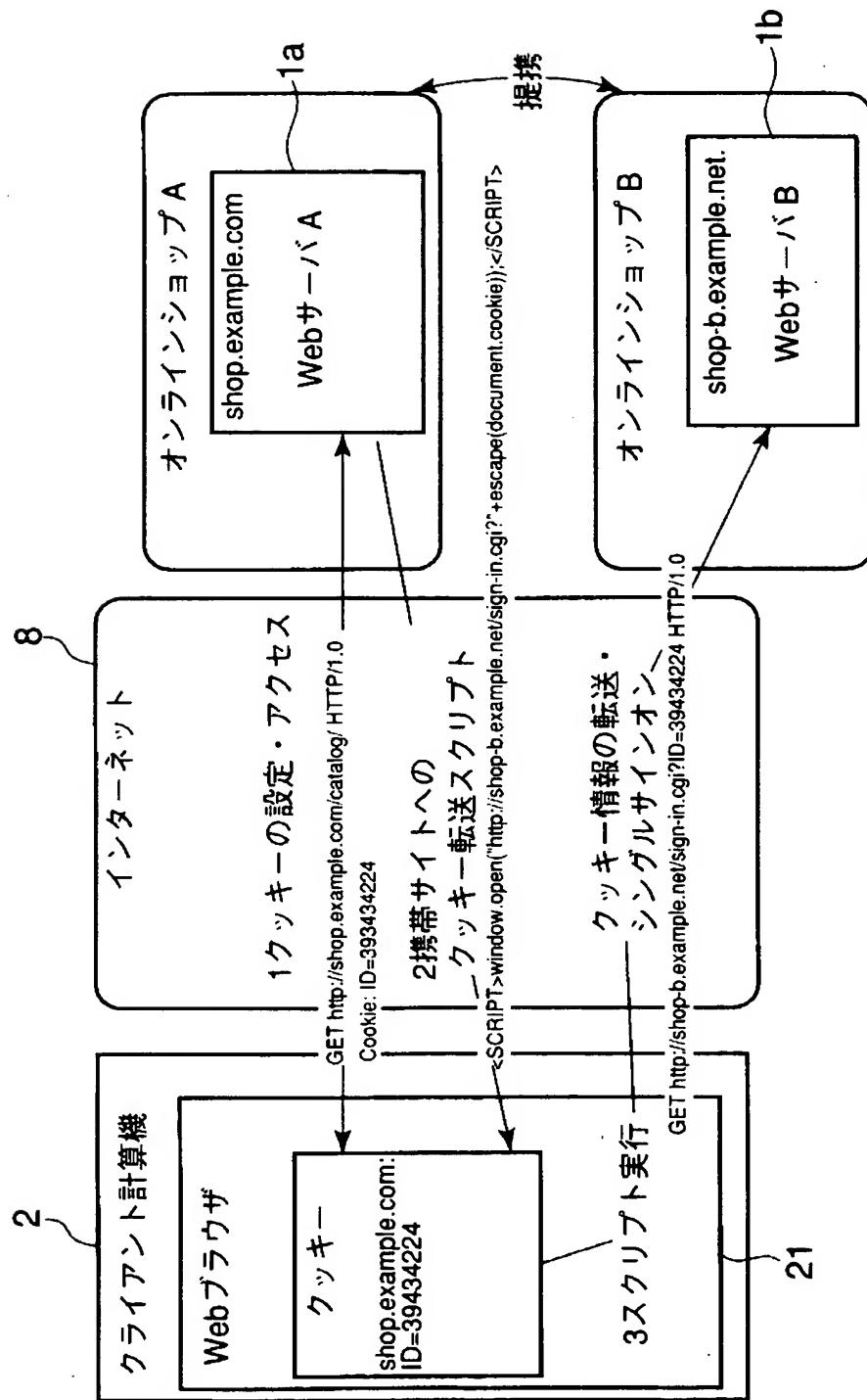
## 3511 クッキー転送許可リスト

http://www.company-a.com/  
 http://www.shop-b.co.jp/login/  
 http://www.service-c.net/shop/  
 :  
 :

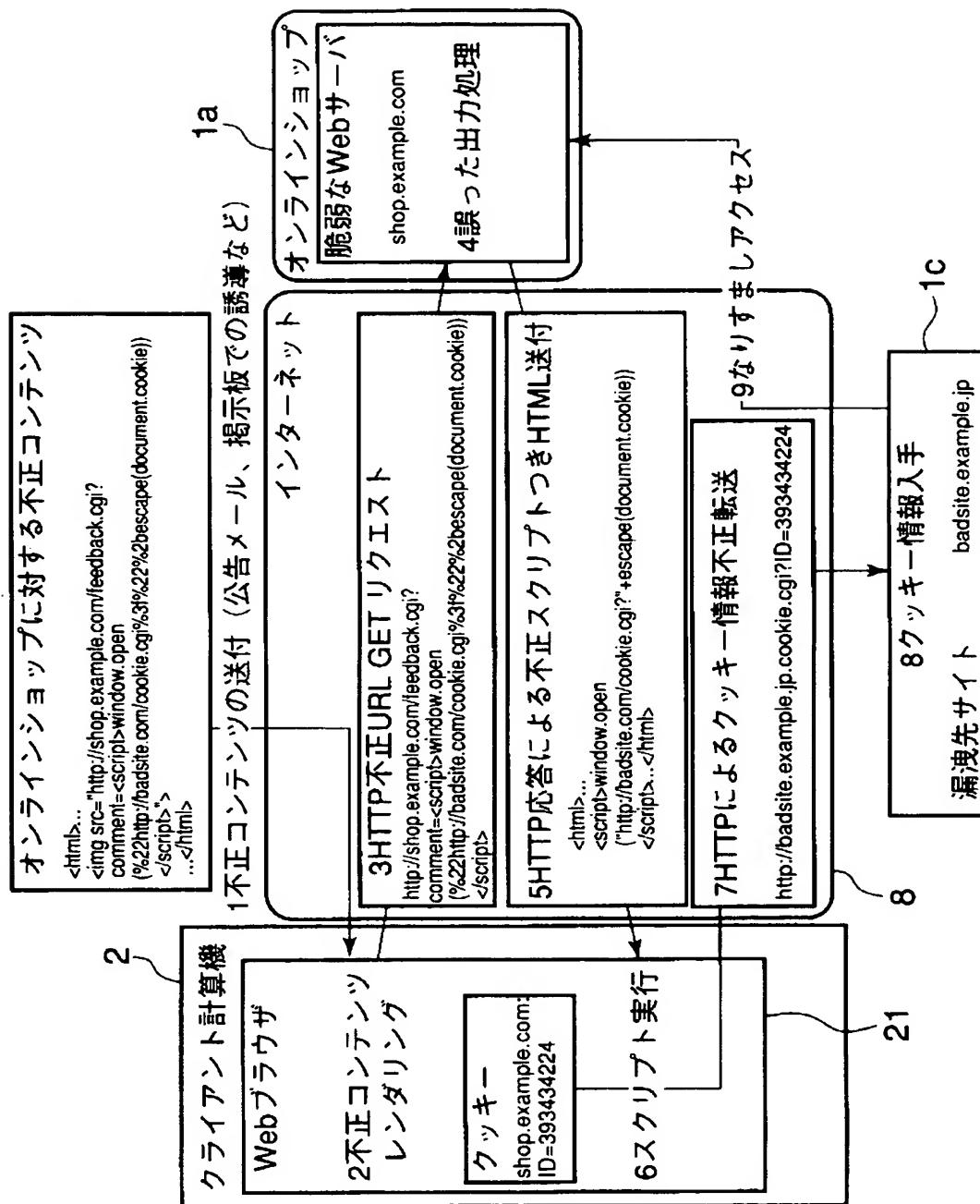
【図 4】



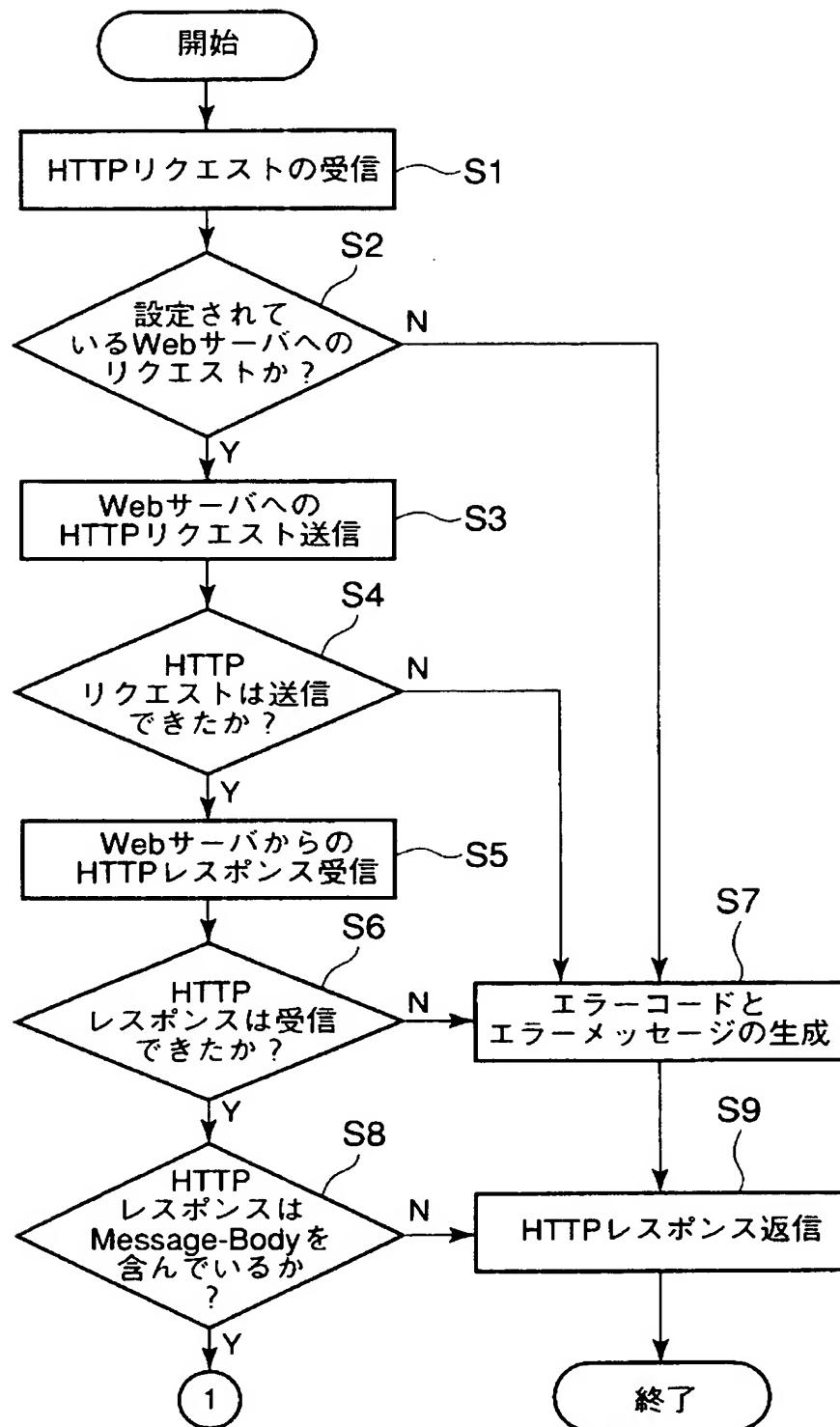
【図 5】



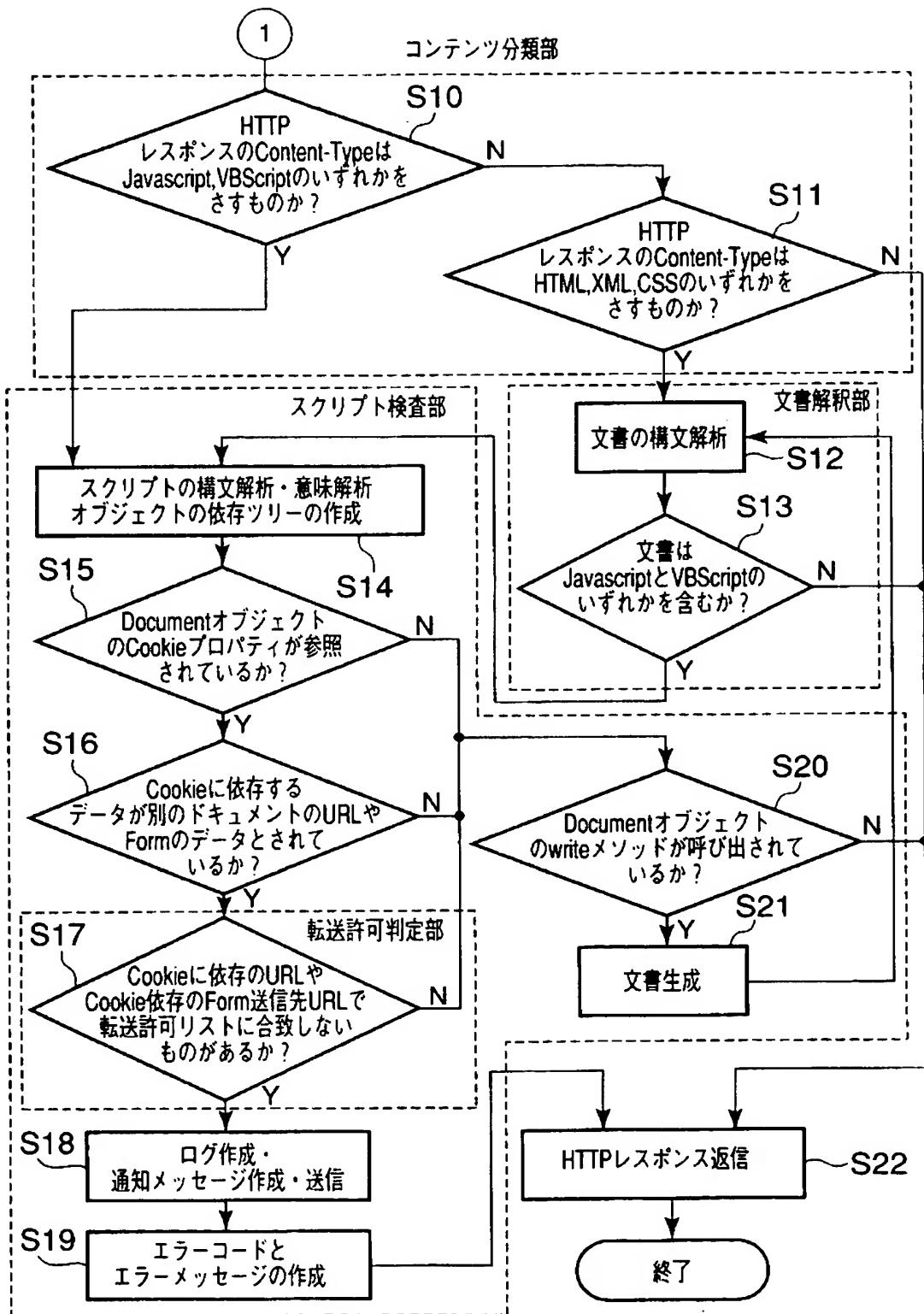
【図 6】



【図7】



【図 8】



【書類名】 要約書

【要約】

【課題】 サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することのできる通信中継装置を提供すること。

【解決手段】 プロキシサーバ3は、Webサーバ1からWebブラウザ21へ転送されるコンテンツを受信すると、このコンテンツから、Webブラウザ21に格納されているクッキー情報をクライアント計算機2から外部の送信先へ向けて送出させる機能を有するスクリプトプログラムを抽出する。そのようなスクリプトプログラムが受信された場合、このコンテンツをクライアント計算機2へ転送してよいかどうかについての許否を判断し、転送が許可されたときにのみ、このコンテンツをクライアント計算機2へ転送する。

【選択図】 図1

特願 2003-096946

出願人履歴情報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日

[変更理由] 住所変更

住 所 東京都港区芝浦一丁目1番1号  
氏 名 株式会社東芝